**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions and listings of the claims in the application:

1.-49. (Canceled)

50. (Currently Amended) A method ~~as in claim 45,~~ including the following:

at a certification authority, receiving an executable program generated by a party independent of the certification authority;

at the certification authority, testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program;

at the certification authority, generating a digital certificate certifying that the executable program operates in the manner described in the specification;

receiving the executable program at a user site;

receiving the digital certificate at the user site;

at the user site, evaluating the digital certificate to determine if the digital certificate is associated with the executable program;

at the user site, evaluating the digital certificate to determine whether to execute the executable program; and

at the user site, executing the executable program, the execution being dependent on the evaluation of the digital certificate, and in which the user site includes a tamper-resistant execution space, the tamper-resistant execution space being operable to protect against tampering, by a user at the user site, with the performance of said step of evaluating the digital certificate to determine whether to execute the executable program.

51. (Canceled)

52. (Currently Amended) A method ~~as in claim 45,~~ including the following:

at a certification authority, receiving an executable program generated by a party independent of the certification authority;

at the certification authority, testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program;

at the certification authority, generating a digital certificate certifying that the executable program operates in the manner described in the specification;

receiving the executable program at a user site in encrypted form;

receiving the digital certificate at the user site;

at the user site, evaluating the digital certificate to determine if the digital certificate is associated with the executable program;

at the user site, evaluating the digital certificate to determine whether to execute the executable program;

decrypting the executable program; and

at the user site, executing the executable program, the execution being dependent on the evaluation of the digital certificate, and in which the user site includes a tamper-resistant execution space, the tamper-resistant execution space being operable to protect against tampering, by a user at the user site, with the performance of said steps of (i) decrypting the executable program, and (ii) evaluating the digital certificate to determine whether to execute the executable program.

53. (Currently Amended) A method ~~as in claim 50~~, including the following:

at a certification authority, receiving an executable program generated by a party independent of the certification authority;

at the certification authority, testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program;

at the certification authority, generating a digital certificate certifying that the executable program operates in the manner described in the specification;

receiving the executable program at a user site;

receiving the digital certificate at the user site;

at the user site, evaluating the digital certificate to determine if the digital certificate is associated with the executable program;

at the user site, evaluating the digital certificate to determine whether to execute the executable program; and

at the user site, executing the executable program, the execution being dependent on the evaluation of the digital certificate, and in which the user site includes a tamper-resistant execution space, the tamper-resistant execution space being operable to protect against tampering, by a user at the user site, with the performance of said step of evaluating the digital certificate to determine whether to execute the executable program, and in which the tamper-resistant execution space includes a secure processing unit.

54.-63. (Canceled)